(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 881 560 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.12.1998 Bulletin 1998/49

(51) Int. Cl.[6]: **G06F 1/00**, G06F 3/06

(21) Application number: **98109862.7**

(22) Date of filing: **29.05.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **29.05.1997 JP 140029/97**

(71) Applicant: **Hitachi, Ltd.**
Chiyoda-ku, Tokyo 101-8010 (JP)

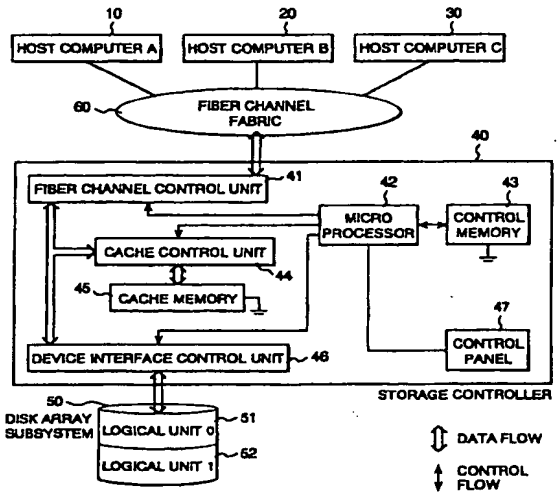
(72) Inventors:
- **Sanada, Akemi**
  Minamiashigara-shi Kanagawa-ken 250-0113 (JP)
- **Nakano, Toshio**
  Chigasaki-shi, Kanagawa-ken 253-0022 (JP)
- **Iwasaki, Hidehiko**
  Hiratsuka-shi, Kanagawa-ken 254-0905 (JP)
- **Sato, Masahiko**
  Odawara-shi, Kanagawa-ken 250-0217 (JP)
- **Muraoka, Kenji**
  Odawara-shi, Kanagawa-ken 250-0866 (JP)
- **Takamoto, Kenichi**
  Odawara-shi, Kanagawa-ken 250-0874 (JP)
- **Kobayashi, Masaaki**
  Odawara-shi, Kanagawa-ken 256-0816 (JP)

(74) Representative:
Strehl Schübel-Hopf & Partner
Maximilianstrasse 54
80538 München (DE)

(54) Fibre channel connection storage controller

(57) N_Port_Name information capable of distinctly identifying a host computer has seen set in a microprocessor 42 of a storage controller 40 prior to start-up of host computers 10, 20, 30; upon startup of the host computers 10, 20, 30, when the storage controller 40 receives a frame issued, then the microprocessor 42 operates to perform comparison for determining whether the N_Port_Name information stored in the frame has been already set in the microprocessor 42 and registered to the N_Port_Name list within a control table maintained. When such comparison results in match, then continue execution of processing based on the frame instruction; if comparison results in failure of match, then reject any request.

FIG. 1



EP 0 881 560 A2

And, by arranging the control table to be stored in a non-volatile control memory, it becomes possible to protect the management information even upon occurrence of any possible power supply failure or interruption.

In accordance with another practical feature of the present invention, after start-up of the host computer, the host computer generates and issues a frame that stores therein N_Port_Name information to the storage control device; the storage control device has means for comparing, when the storage control device receives this information, the maintained N_Port_Name information for distinct identification of the host computer to the N_Port_Name information as stored in the received frame: If the comparison results in a match between the two, then continue to execute the processing based on an instruction of the frame received; alternatively, if the comparison tells failure in match then return to the host computer an LS_RJT frame which rejects the presently received frame. It is thus possible for the storage control device to inhibit or deter any unauthorized access from the host computer.

A further practical feature of the present invention lies in presence of a means for setting N_Port_Name information items which are greater in number than or equal to a physical number of host interface units (ports) as owned by the storage control device. More specifically, a means is specifically provided for setting a plurality of N_Port_Name information items per port. This makes it possible to accommodate a multi-logical path configuration upon either a fiber channel fabric or a multi-logical path configuration upon switch connections.

Further, in a system having many magnetic disk volume parts such as a disk array device and also having a plurality of channel path routes, the system has manager means for performing management--within the storage control device in a one-to-one correspondence relation per channel path route--of storage regions under control of the storage control device, including a logical unit number (LUN)-based logical disk extent, a physical volume extent, a RAID group-based logical disk extent and the like, versus ports of the storage control device and N_Port_Name information of a host computer(s). This may enable users to deter an unauthorized access attempt per storage region, which in turn leads to achievement of more precise access management.

Furthermore in the present invention, even where the storage device under control of the storage control device is any one of an optical disk drive, magneto-optical (MO) disk drive and magnetic tape device as well as a variety of types of library devices of them, the storage control device has means for performing table based management and the storage information of a control table-based manager/holder means for dealing with the correspondence among the N_Port_Name information of an accessible host computer, ports of the storage control device, and the storage device, and further handling the correspondence management of media in the case of library apparatus, while simultaneously having a means for comparing, upon receipt of a frame as sent thereto, the information within the frame to the information in the control table, thereby eliminating unauthorized access attempts from host computers.

Moreover, the present invention comprises means for protecting the management information through inputting of a password upon setup of the information under management of the storage control device using a panel or the like. With such an arrangement, it is possible for users to eliminate any fraudulent registration of the information and also unauthorized resetting of the same. In addition, the users are capable of readily deter any unauthorized access by merely setting such management information thus reducing workloads on the users.

It should be noted that in the present invention, the means for setting the information as managed by the storage control device may be designed so that the use of the panel or the like is replaced with use of a utility program or programs of host computers to attain the intended setup operation.

In accordance with the present invention, in a computer system employing the ANSIX3T11-standardized fiber channel as the interface between host computers and a storage control device and also including the host computers, the storage control device and more than one storage device under control of the storage control device, it is possible to deter unauthorized access from any one of the host computers, which in turn makes it possible to attain the intended data secrecy protection within the storage device.

In addition, it becomes possible to precisely managing those access attempts from any one of the host computers in a one-to-one correspondence manner among the host computers and storage controller ports as well as storage regions; accordingly, the storage device may be efficiently utilized to meet the needs upon alteration of the usage per storage region.

These and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments of the invention, as illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a diagram showing a hardware configuration of a first practicing form of the present invention.

Fig. 2 is a diagram showing a format of a frame in the first practicing form.

Fig. 3 is a diagram showing a format of a frame header which constitutes the frame shown in Fig. 2.

Fig. 4(A) is a format diagram of a payload of FCP_CMND which is one of frames shown in Fig. 2; and, Fig. 4(B) is a format diagram of FCP_CDB constituting the payload.

Fig. 5 shows one example of a sequence perform-

interface controller 46 thus permitting data and redundancy data to be written into the disk array subsystem 50. In this case, during ordinary or standard RAID5 operations, a new parity is created based on the old data and old parity as well as new data; on the contrary, according to the control scheme of this invention, the microprocessor 42 does the same using the device interface controller 46 and the cache control unit 44 as well as the control memory 43 plus the cache 45.

On the other hand, upon receipt of read command information as the command information from the host computer 10, the microprocessor 42 sends an instruction to the device interface control unit 46 for providing access to the disk array subsystem 50 which stores therein the data block of this access request to read data therefrom, which data will then be stored into the cache 45 through the cache control unit 44. The microprocessor 42 issues an instruction to the fiber channel control unit 41; the fiber channel control unit 41 in turn transfers the data stored in the cache 45 toward the host computer 10 and then sends a read completion report to the host computer after completion of the data transfer required.

Next, a technical advantage of the fiber channel 60 will be explained as follows. The fiber channel may be a high-speed interface capable of transferring data at 100 MB/s at a distance of 10km in maximum. The fiber channel's architecture is designed to send data from a "source" buffer to its "destination" buffer while moving the buffer contents from one device to another in a way independent of the format and contents of data per se; accordingly, any overhead which processes different network communications protocols will no longer take place thus enabling achievement of high-speed data transmission. A variety of kinds of layers may be built in the upper-level logical layer, such as for example TCP/IP, SCSI, ESCON, IPI and the like. In other words, it does have the logical compatibility with other interfaces. The device called the fabric is expected to execute the complicated device-to-device connection/exchange function, which leads to the capability of organization of a multi-layered logical bus configuration.

The basic unit based on which the fiber channel exchanges or distributes data is called the "frame." Next, this frame will be explained with reference to Fig. 2.

As shown in Fig. 2, a frame 70 is configured from a start-of-frame (SOF) section 71, frame header 72, data field 73, cyclic redundancy check (CRC) 74, and end-of-frame (EOF) 75.

The SOF 71 is an identifier of 4 bytes which is put at the top of the frame.

The EOF 75 is a 4-byte identifier at the last location of the frame; a combination of SOF 71 and EOF 75 indicates the boundary of frame. In the fiber channel, an "idle" signal or signals flow therein in cases where any frames are absent.

The frame header 72 contains therein a frame type, host protocol type, source and destination's N_Port_ID information, N_Port_Name information and the like. The N_Port_ID is information indicative of an address, whereas N_Port_Name represents a port identifier.

The header of upper-level layer may be put at the top part of the data field 73. This is followed by a payload section which carries data per se. CRC 74 is a 4 byte check code for use in checking or verifying the frame header and data in the data field.

The frame header 72 has a format 80 as shown in Fig. 3. In the frame header format 80, a destination identifier (D_ID) 81 is an address identifier on the frame reception side, whist a source identifier (S_ID) 82 is an identifier indicative of the N_Port address on the frame transfer side, each of which may involve N_Port_ID, N_Port_Name information, etc.

An explanation will next be given of a payload 90 of fiber channel protocol command FCP_CMND, which stands for fiber channel protocol for SCSI command and which is one of payloads of the data field 73 constituting the frame, in conjunction with Figs. 4(A) and 4(B).

A logical unit number LUN for issuance of a command is assigned to an FCP logical unit number (FCP_LUN) field 91. A command control parameter is assigned to an FCP control (FCP_CNTL) field 92. And, an SCSI command descriptor block is stored in an FCP command descriptor block (FCP_CDB) field 93 for indication of a command type such as a read command "Read" or the like, an address such as LUN, and a block number. The amount of data to be transferred in response to the command is designated by byte number in an FCP data length (FCP_DL) field 94.

Data exchange/distribution operations are executed by use of the frame thus arranged as described above.

Frames employed herein may be generally classified based on function into a data frame and link control frame. The data frame is for use in transferring information, and thus has data and command as used by the host protocol, which are built in the payload section of the data field thereof.

On the other hand, the link control frame is typically used for indication of a success or failure of frame distribution. There may be a frame or the like for use in indicating actual receipt of a single frame or in notifying a parameter concerning transmission in log-in events.

Next, the "sequence" will be explained with reference to Fig. 5. The sequence in the fiber channel may refer to a collection of data frames concerned which will be unidirectionally transferred from one N_Port to another N_Port, the sequence corresponding to the phase in SCSI. A collection of such sequences is called the "exchange." One example is that a collection or group of certain sequences will be called the exchange, which sequences undergo exchange/distribution processing for execution of a command within a time period spanning from the issuance of such command to the completion of command execution (including com-

will possibly be altered or modified and is not the numeral value under management by the users.

Next, an explanation will be given of a frame processing procedure of the storage controller in reply to issuance of a log-in request from a host computer with reference to Figs. 1 and 7.

(Step S71)

The host computers 10, 20, 30 start up each issuing a PLOGI frame, which is the log-in request frame storing therein the N_Port_Name information. Upon receipt of such frame, the microprocessor 42 of the storage controller 40 sends back each host computer an ACK frame representative of actual receipt of the frame.

(Step S72)

And, the microprocessor 42 attempts to extract N_Port_Name information as stored in the frame, and then performs comparison for determining whether such N_Port_Name information has already been registered in the N_Port_Name list within the presently available preset control table.

(Step S73), (Step S74), (Step S75)

The N_Port_Name information that is presently stored in the frames issued from the host computers 10, 20 may match the N_Port_Name information which has been registered within the control table so that the microprocessor 42 of the storage controller 40 returns the ACC frame to the host computers 10, 20 as a mark of actual receipt of the individual log-in request while simultaneously continuing to execute the log-in processing.

(Step S73), (Step S76)

On the other hand, the N_Port_Name information stored in the frame as issued from the remaining host computer 30 fails to match the N_Port_Name information registered in the control table so that the microprocessor 42 of storage controller 40 returns to the host computer 30 an LS_RJT frame which contains therein a reject parameter for rejection of its connection attempt.

In the way as described above, by causing the storage controller 40 to manage the one-to-one correspondence of those ports of the host computers and the storage controller using the log-in request control table 130, it is possible for users to prevent any unauthorized access attempts from host computers on a port-by-port basis thereby maintaining enhanced security.

Next, one preferred methodology will be described which is for practicing the security check scheme using the N_Port_Name information per LUN that is the storage region of the disk array subsystem in accordance with the principles of the present invention.

In accordance with the invention, first establish a list of those accessible host computers per LUN to the microprocessor 42 of storage controller 40 before startup of the host computers 10, 20, 30. Then, input using the panel 47 certain information such as the N_Port_Name or N_Port_ID information or the like capable of identifying the host computers. When this is done, request entry of a password upon inputting of such information in order to achieve the secrecy protection function through input to the panel 47, thereby enhancing the security.

After inputting such password, if this matches the preset password, then input the port of storage controller along with the N_Port_Name information of one or several accessible host computers, thereby storing the input information in the control table.

Assume here that the LU0 (51) is accessible from the host computer 10 via a port of the fiber channel control unit 41 of the storage controller 40 whereas the LU1 (52) is accessible from the host computer 20 via a port of fiber channel control unit 41 of storage controller 40. Suppose that regarding the N_Port_Name, the host computer 10 is HOSTA while host computer 20 is HOSTB. Imagine that a port of fiber channel control unit 41 of storage controller 40 is CTL0P0. If this is the case, an I/O request control table 140 is as shown in Fig. 8.

This I/O request control table 140 shown in Fig. 8 is established in the storage space of a nonvolatile memory thereby making it possible to protect the management information against loss or destruction due to any accidental power interruption or failure.

In addition, upon occurrence of power off, the information stored in the I/O request control table 140 shown in Fig. 8 is to be stored in the hard disk region 50. Or alternatively, reflection is carried out to the memory 43 and disk 50 upon updating of information. This makes it possible to permanently hold or maintain the information until it is reestablished at later stages.

Although in this embodiment the channel path route is single, the same goes with other systems having a plurality of channel path routes.

A frame processing procedure of the storage controller in response to issuance of the I/O request from more than one host computer will now be explained in conjunction with Figs. 1 and 9. While in the prior example stated supra the security check was done in the course of PLOI, the check is performed per SCSI command in this embodiment.

(Step S91)

Where the host computer 10 desires to issue the I/O request to LU0 (51), the host computer 10 generates and issues a specific frame storing therein SCSI CDB toward the storage controller 40. Upon receiving of this frame, the storage controller 40 first sends back the ACK frame representative of actual receipt of this frame.

startup of the host computer, the host computer generates and issues to the storage control device a frame storing therein N_Port_Name information; the storage control device has means for comparing, upon receipt of this information, the N_Port_Name information distinctly identifying the host computer as already set and stored therein to the N_Port_Name information presently stored in a received frame; and, a fiber channel connection storage control device has means for eliminating unauthorized access from the host computer in a way such that when the comparison results in match, processing based on an instruction of the frame is continued, and when failed to match, a link service reject (LS_RJT) frame for rejection of the received frame is returned to the host computer.

2. In a computer system including a host computer, a storage device having a magnetic disk drive, and a fiber channel connection storage controller employing an ANSIX3TT11-standardized fiber channel as an interface between the host computer and the storage device, the magnetic disk drive being operable under control of the fiber connection storage controller, the fiber channel connection storage controller comprising;

N_Port Name information which is information as issued from the host computer to distinctly identify the host computer is preinstalled in the storage control device prior to startup of the host computer; the storage control device has means for permanently storing therein the information until this information will be reset; after startup of the host computer, the host computer generates and issues to the storage control device a frame storing therein N_Port_Name information; the storage control device has means for comparing, upon receipt of this information, the N_Port_Name information distinctly identifying the host computer as already set and stored therein to the N_Port_Name information presently stored in a received frame; a fiber channel connection storage control device has means for eliminating unauthorized access from the host computer in a way such that when the comparison results in match, processing based on an instruction of the frame is continued, and when failed to match, a link service reject (LS_RJT) frame for rejection of the received frame is returned to the host computer; and, the fiber channel connection storage control device also has means for setting N_Port_Name information items greater in number than or equal to a physical number of host interfaces (ports) as owned by the storage control device, that is, means for setting a plurality of N_Port_Name information items per port, and means for deterring unauthorized access from the host computer even for a multi-logical path configuration upon a fiber channel Fabric connection.

3. In a computer system including a host computer, a storage device having a magnetic disk drive, and a fiber channel connection storage controller employing an ANSIX3TT11-standardized fiber channel as an interface between the host computer and the storage device, the magnetic disk drive being operable under control of the fiber connection storage controller, the fiber channel connection storage controller comprising;

N_Port Name information which is information as issued from the host computer to distinctly identify the host computer is preinstalled in the storage control device prior to startup of the host computer; the storage control device has means for permanently storing therein the information until this information will be reset; after startup of the host computer, the host computer generates and issues to the storage control device a frame storing therein N_Port_Name information; the storage control device has means for comparing, upon receipt of this information, the N_Port_Name information distinctly identifying the host computer as already set and stored therein to the N_Port_Name information presently stored in a received frame; a fiber channel connection storage control device has means for eliminating unauthorized access from the host computer in a way such that when the comparison results in match, processing based on an instruction of the frame is continued, and when failed to match, a link service reject (LS_RJT) frame for rejection of the received frame is returned to the host computer; and, the fiber channel connection storage control device also has means for setting N_Port_Name information items greater in number than or equal to a physical number of host interfaces (ports) as owned by the storage control device, that is, means for setting a plurality of N_Port_Name information items per port, and means for deterring unauthorized access from the host computer even for a multi-logical path configuration upon a fiber channel Fabric connection; and

further characterized in that in a system having many magnetic disk volumes as in a disk array device under control of the storage control device and also having a plurality of channel path routes, the fiber channel connection stor-

FIG. 1

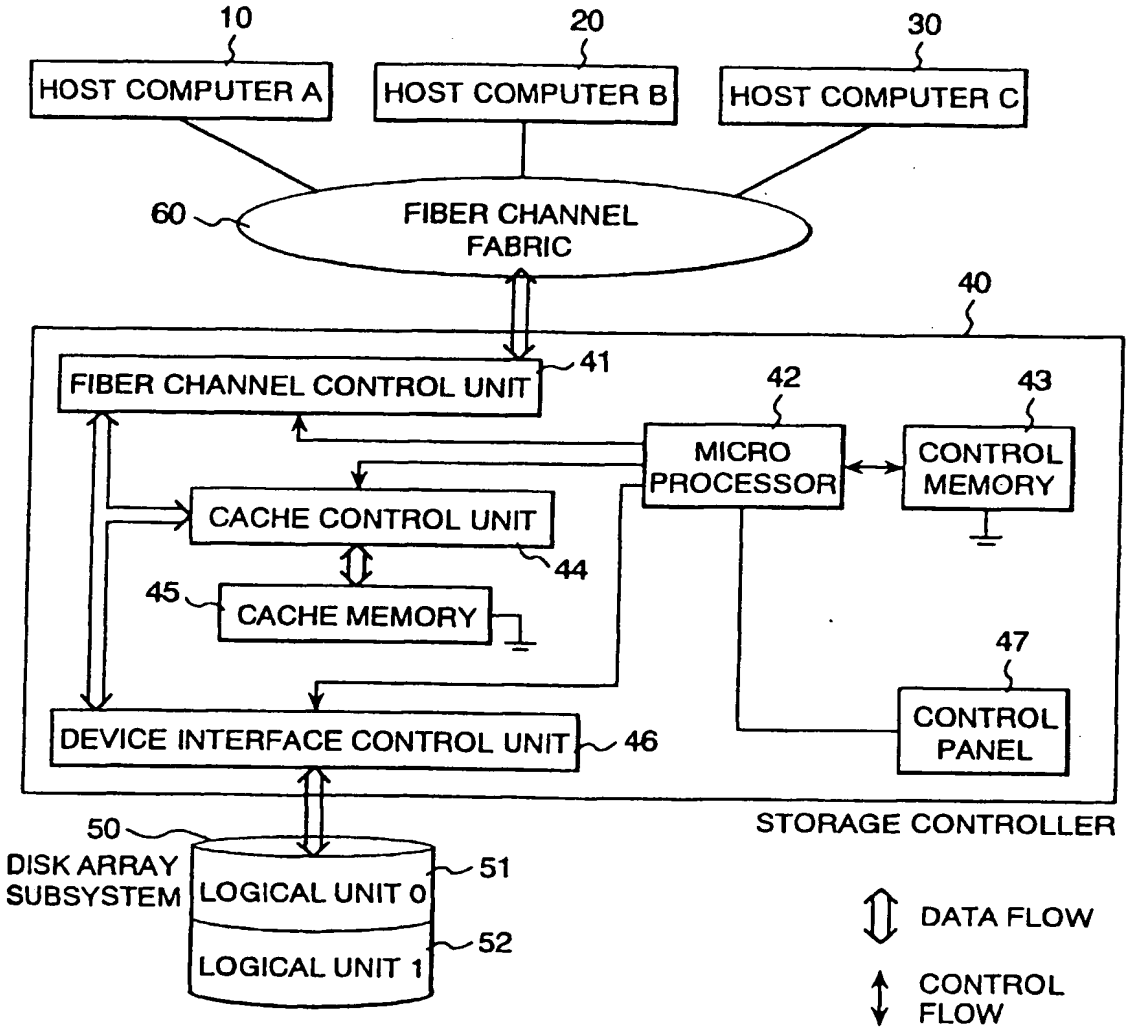


FIG. 3

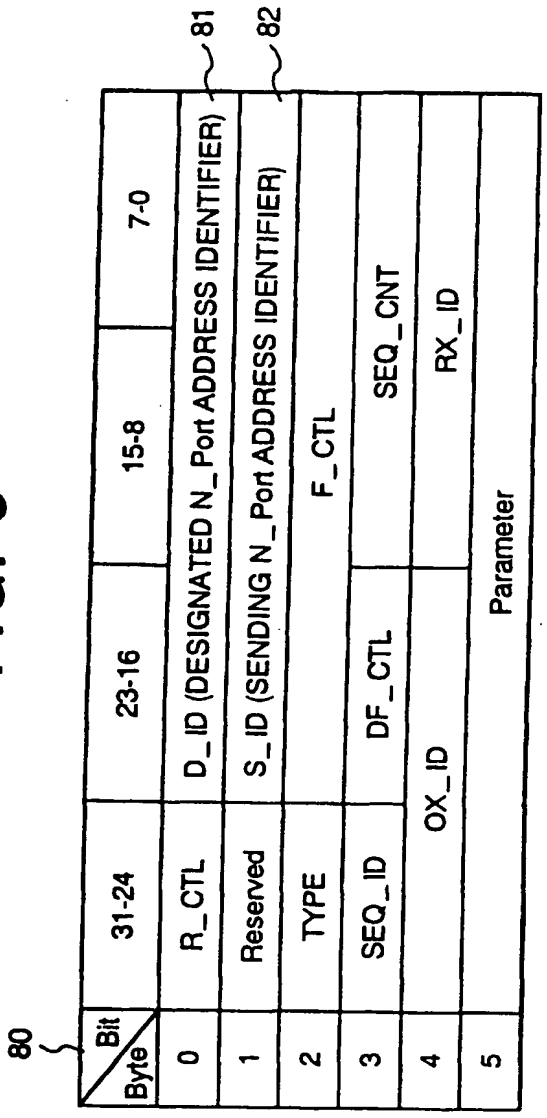


FIG. 5A

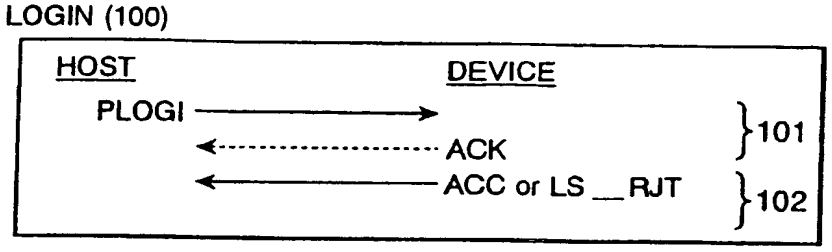


FIG. 5B

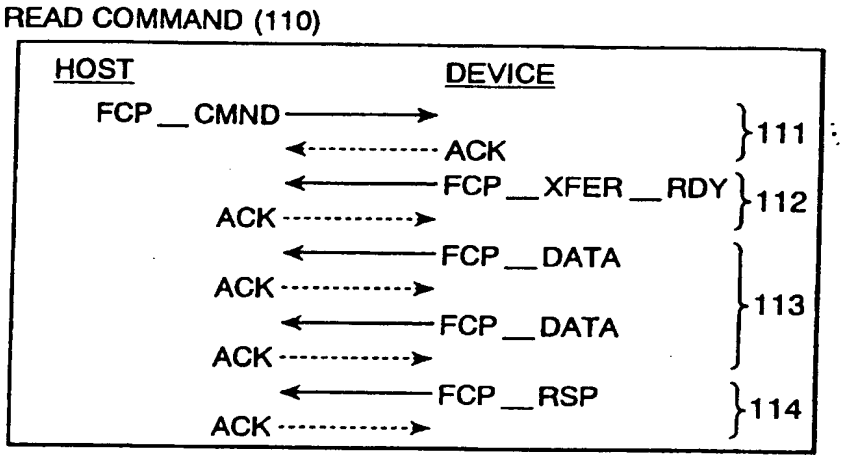


FIG. 5C

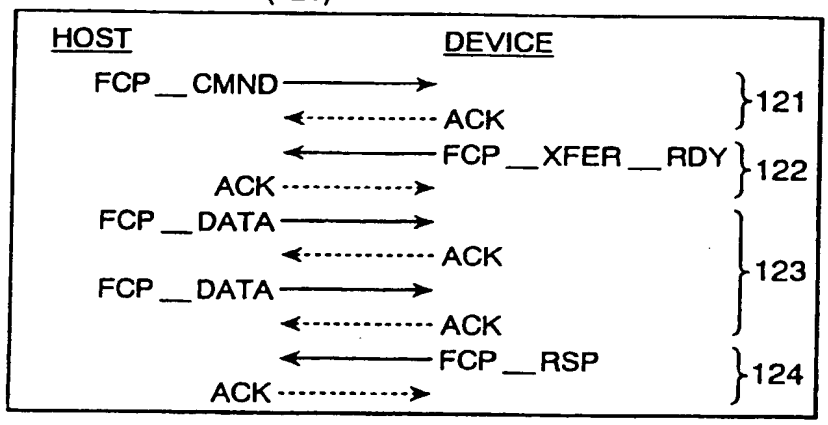


FIG. 7

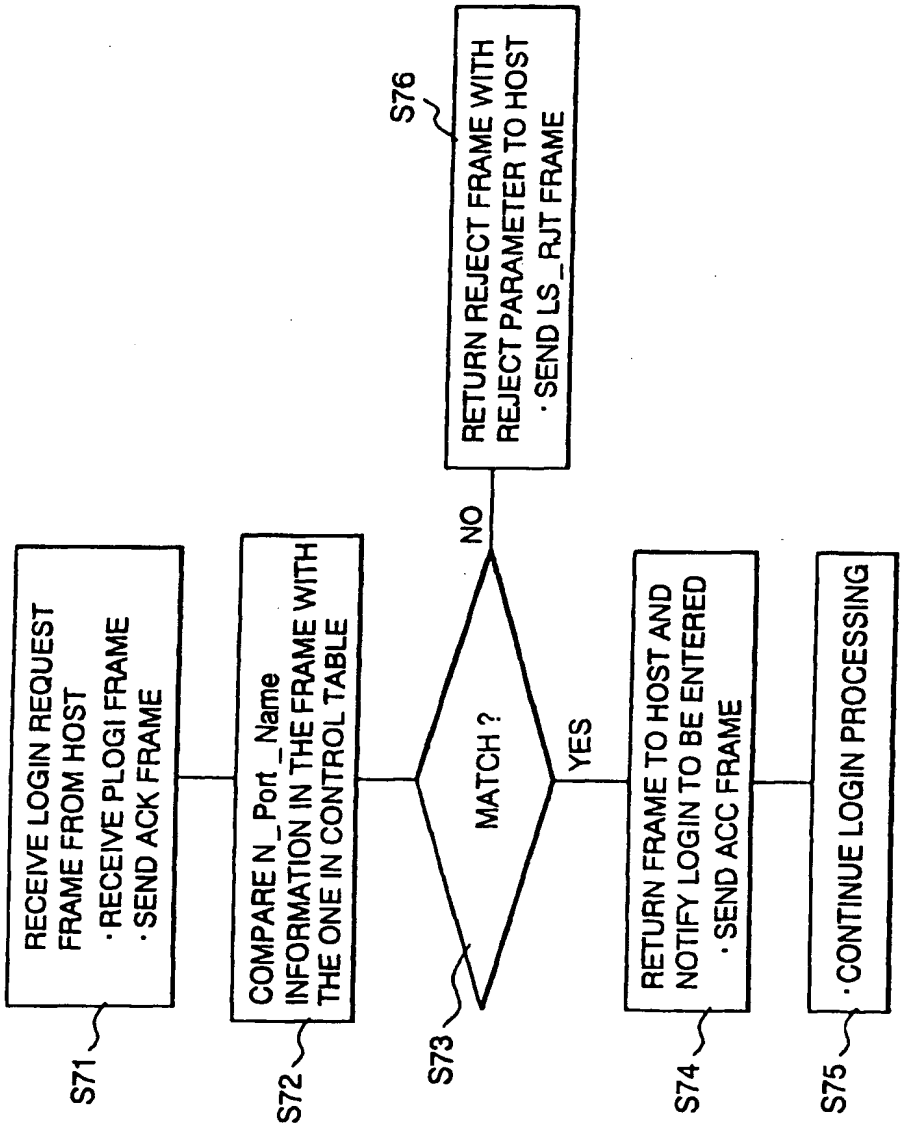


FIG. 9

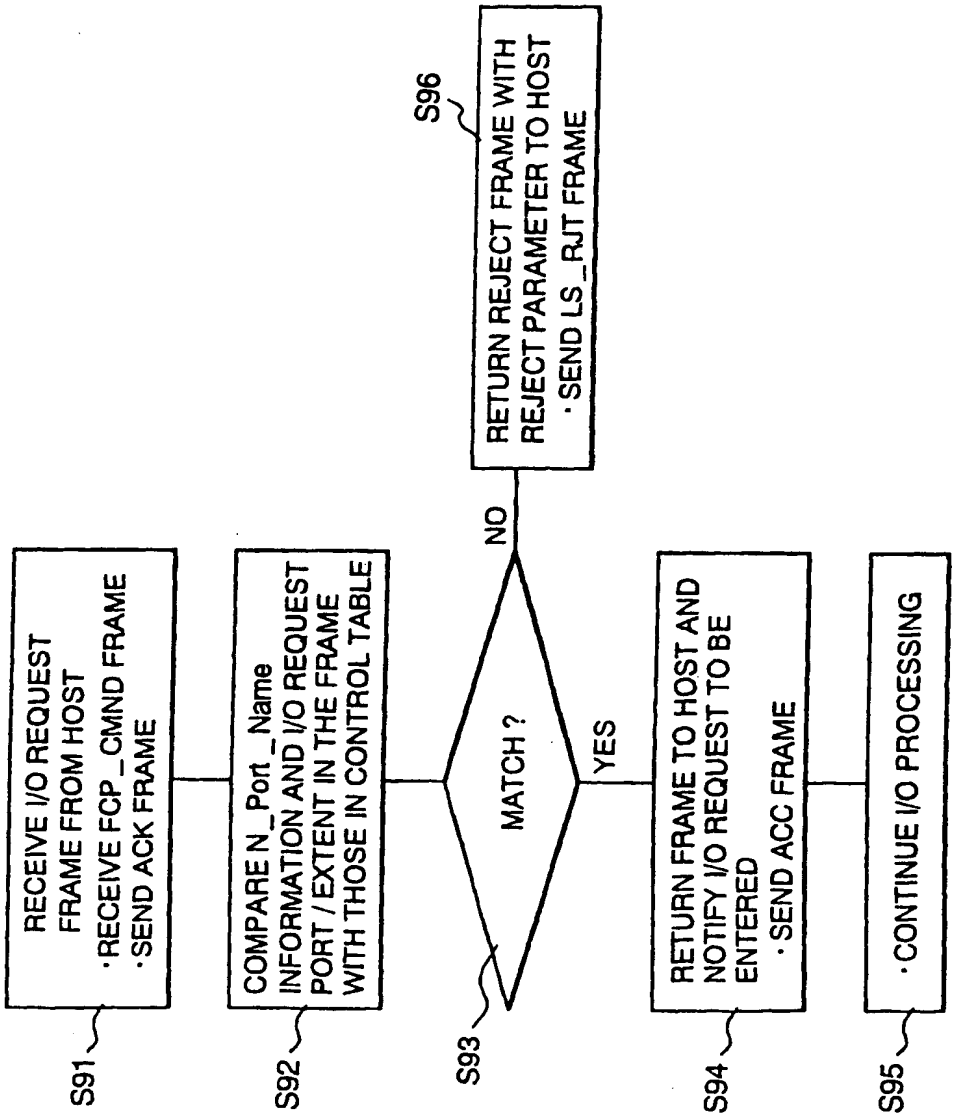


FIG. 11

CONTROL TABLE 160

STORAGE REGION OPTICAL DISK MEDIUM	OPTICAL DISK DRIVE	HOST N__Port__Name	HOST INTERFACE (OR PORT) ON STORAGE CONTROLLER
MEDA	DRIVE0	HOSTA	CTL0P0
MEDB	DRIVE0	HOSTA	CTL0P0
MEDC	DRIVE0	HOSTA	CTL0P0
MEDD	DRIVE0	HOSTB	CTL0P0
MEDE	DRIVE0	HOSTB	CTL0P0